BLACKBIRD FOR TRAINING

شهادة أمن المعلومات في مدفوعات فيزا

June 2027 24 – 20

عمّان (الأردن)



شهادة أمن المعلومات في مدفوعات فيزا

المرجع: 194102_3255353 **التاريخ:** 20 – 24 June 2027 **المكان:** عمان (الأردن) **الرسوم:** GBP 4900

المقدمة

في ظل التطور المتسارع في أنظمة الدفع الرقمي والاعتماد المتزايد على تقنيات المعاملات الإلكترونية، أصبحت حماية بيانات المدفوعات من أولويات المؤسسات المالية والتجارية حول العالم. تمثل شهادة أمن المعلومات في مدفوعات فيزا معيارًا احترافيًا معتمدًا يهدف إلى رفع كفاءة المتخصصين في مجال الأمن السيبراني وفهمهم العميق لآليات حماية نظم المدفوعات الإلكترونية.

تتيح هذه الشهادة للمشاركين تطوير قدراتهم في تقييم المخاطر، وتصميم استراتيجيات وقاية فعالة، والالتزام بالمعايير الدولية لأمن البيانات. تستهدف الدورة المديرين، وقادة الفرق، والمتخصصين في مجالات الأمن السيبراني، والخدمات المالية، وإدارة المخاطر، إضافةً إلى العاملين في أقسام تكنولوجيا المعلومات الذين يسعون لتعزيز جاهزية مؤسساتهم ضد التهديدات الرقمية الحديثة.

تمنح هذه الدورة فهماً عملياً وعميقاً حول كيفية بناء بيئة دفع آمنة وموثوقة، وتمكّن المشاركين من تطبيق ضوابط الحماية بشكل احترافي يحقق الامتثال لأعلى المعايير العالمية في مجال أمن المدفوعات.

أهداف الدورة

- التعرف على المعايير العالمية الخاصة بأمن المدفوعات الإلكترونية.
- فهم الهيكل التنظيمي لمنظومة أمن فيزا وأدوارها التشغيلية.
- تطبيق استراتيجيات الحماية والوقاية من الاختراقات السيبرانية.
- تحليل المخاطر المتعلقة بالمدفوعات الرقمية وتقييم تأثيرها المؤسسي.
- إعداد خطط استجابة فعالة للحوادث الأمنية.
- تطوير قدرات الرقابة الداخلية والامتثال التنظيمي.
- تطبيق الضوابط التقنية للحماية من الاحتيال المالي والهجمات الإلكترونية.
- تحسين كفاءة الاتصال الداخلي بين فرق الأمن السيبراني والإدارات الأخرى.



محاور الدورة

اليوم الأول: أساسيات أمن المدفوعات الإلكترونية

- مقدمة في مفاهيم الأمن السيبراني.
- التعرف على بنية نظام فيزا للمدفوعات.
- تحليل دورة حياة المعاملة الإلكترونية.
- تحديد النقاط الحرجة المحتملة للاختراق.
- استعراض لأبرز الهجمات السيبرانية في مجال المدفوعات.
- تمارين تطبيقية في تحليل الثغرات الأمنية.

اليوم الثاني: إدارة المخاطر والضوابط التنظيمية

- تعريف إطار عمل إدارة المخاطر في أنظمة الدفع.
- منهجيات تقييم المخاطر المؤسسية.
- الضوابط الإدارية والتقنية المعتمدة في نظام فيزا.
- الامتثال لمعايير PCI DSS وأهم بنودها.
- إعداد تقارير تحليل المخاطر.
- تمارين جماعية لتصميم خطة إدارة مخاطر فعالة.

اليوم الثالث: الحماية التقنية للبنية التحتية للمدفوعات

- تأمين الشبكات وأنظمة الخوادم الخاصة بالمدفوعات.
- إدارة مفاتيح التشفير وتطبيق تقنيات المصادقة القوية.
- مراقبة الأنشطة غير الاعتيادية وتحليل السجلات الأمنية.
- أدوات الكشف المبكر عن التهديدات.
- تطبيقات الذكاء الاصطناعي في كشف الاحتيال.
- تمرين عملي لمحاكاة هجوم إلكتروني على نظام دفع.



اليوم الرابع: الاستجابة للحوادث والتعافي من الاختراقات

- مبادئ إدارة الحوادث الأمنية.
- خطوات الاستجابة الفورية للحوادث.
- تحليل الأدلة الرقمية وتوثيق الحادثة.
- وضع خطة لاستمرارية الأعمال.
- تنسيق فرق العمل خلال الطوارئ.
- ورشة تطبيقية لتصميم خطة استجابة مؤسسية.

اليوم الخامس: الامتثال والتقييم النهائي

- مراجعة شاملة لمتطلبات شهادة فيزا.
- إعداد التقارير الدورية لأمن المعلومات.
- آليات التقييم الذاتي والاختبار الداخلي.
- إجراءات الاعتماد النهائي من فيزا.
- مناقشة حالات واقعية من بيئات العمل.
- التقييم الختامي والاختبار التطبيقي.

لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات!

- اكتساب خبرة عملية متقدمة في أمن المدفوعات.
- تعزيز فرص الترقية المهنية والاعتماد المؤسسي.
- فهم شامل للمعايير الدولية في أمن نظم الدفع.
- تقوية القدرات التحليلية في تقييم التهديدات.
- بناء ثقافة أمنية فعّالة داخل المؤسسة.
- اكتساب مهارات الامتثال التنظيمي.
- تطوير مهارات التواصل الأمني مع الإدارات الأخرى.
- تعزيز ثقة العملاء والمستثمرين بالمؤسسة.

الخاتمة

تعد شهادة أمن المعلومات في مدفوعات فيزا خطوة استراتيجية لأي محترف يسعى لترسيخ خبرته في مجال الأمن السيبراني وحماية المعاملات الإلكترونية. فهي لا تقتصر على الجانب النظري، بل تدمج المعرفة بالممارسة العملية وتساعد على بناء قدرات حقيقية لمواجهة التحديات الأمنية المعاصرة.



إن تبني المؤسسات لهذا النوع من التدريب يسهم في تعزيز الثقة، وضمان الامتثال، وحماية بيانات العملاء من المخاطر الرقمية. في عالم تتسارع فيه التحولات التقنية، تصبح المعرفة المتخصصة في أمن المدفوعات أحد أعمدة الاستدامة المؤسسية والتميز المهني.

